

UNITED STATES DISTRICT COURT

for the

Western District of North Carolina

In the Matter of the Search of)
 (Briefly describe the property to be searched)
 or identify the person by name and address))

Case No. 3:22-mj-129

A SAMSUNG PHONE, CURRENTLY LOCATED)
 AT FBI CHARLOTTE, 7915 MICROSOFT WAY,)
 CHARLOTTE, NC)

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (*identify the person or describe the property to be searched and give its location*):

A Samsung SM-G998U cellular phone, serial: R3CR70HDQN[last alphanumeric character illegible], IMEI 1: 351600220 located at FBI Charlotte, 7915 Microsoft Way, Charlotte, North Carolina 28273 as further described in Attachment A. located in the Western District of North Carolina, there is now concealed (*identify the person or describe the property to be seized*):

Evidence of, instrumentalities used in committing, and fruits of the crimes pertaining to violations of 18 U.S.C. Section 2252A, as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (*check one or more*):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

<i>Code Section</i>	<i>Offense Description</i>
18 U.S.C. § 2252A(a)(2)(A)	Receipt/Distribution of Child Pornography
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography

The application is based on these facts:

See attached affidavit incorporated by reference herein.

- ☒ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/S/ Michael Gregory

Applicant's signature

Michael Gregory, Special Agent - F.B.I.

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P 4.1 by telephone

Signed: March 18, 2022

W. Carleton Metcalf

W. Carleton Metcalf
 United States Magistrate Judge



Date: 3/18/2022

City and state: Asheville, North Carolina

W. Carleton Metcalf, U.S. Magistrate Judge

Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

IN THE MATTER OF THE SEARCH OF A
SAMSUNG PHONE, CURRENTLY
LOCATED AT FBI CHARLOTTE, 7915
MICROSOFT WAY, CHARLOTTE,
NORTH CAROLINA 28273.

Case No. 3:22-mj-129

**AFFIDAVIT IN SUPPORT OF AN
APPLICATION UNDER RULE 41 FOR A
WARRANT TO SEARCH AND SEIZE**

I, Michael Gregory, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—an electronic device—which is currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation (FBI), and have been employed since April 2012. I am currently assigned to investigate federal crimes against children to include: international parental kidnapping, child abductions, sexual exploitation of children, domestic trafficking of children/prostitution, child sex tourism and national sex offender registry violations. I have received extensive training in investigations as a New Agent Trainee at the FBI Academy in Quantico, Virginia as well as follow on training as it relates to my current assignment. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Probable cause includes information known to me and/or provided to me by other federal, state, and/or local law enforcement officers.

IDENTIFICATION OF THE DEVICE TO BE EXAMINED

4. The property to be searched is a Samsung SM-G998U cellular phone, serial: R3CR70HDQN[last alphanumeric character illegible], IMEI 1: 351600220114740, IMEI 2: 350876360114747, hereinafter the "Device." The Device is currently located at 7915 Microsoft Way, Charlotte, North Carolina 28273.

5. The applied-for warrant would authorize the forensic examination of the Device for the purpose of identifying electronically stored data particularly described in Attachment B.

STATUTORY AUTHORITY

6. This investigation concerns violations of 18 U.S.C. § 2252A relating to material involving the sexual exploitation of minors.

- a. Title 18, U.S.C. § 2252A(a)(2)(A), prohibits the knowing receipt or distribution of (a) any child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including by computer using any means or facility of interstate or foreign commerce shipped or transported in or affecting interstate or foreign commerce by any means, including by computer; or (b) any material that contains child pornography as defined in 18 U.S.C. § 2256(8), using any means or facility of

interstate or foreign commerce or that has been mailed, or has been shipped or transported in or affecting interstate or foreign commerce by any means, including computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

- b. 18 U.S.C. § 2252A(a)(5)(B) prohibits knowingly possessing or knowingly accessing with intent to view, any book, magazine, periodical, film, videotape, computer disk, or any other material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, or shipped or transported using any means or facility of interstate or foreign commerce or in or affecting interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed, or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

DEFINITIONS

- 7. The following definitions apply to this Affidavit:
 - a. “Child Pornography,” is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (a) the production of the visual depiction involves the use of a minor engaged in sexually explicit conduct; (b) such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

(c) such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

- b. “Visual Depictions” include undeveloped film and videotape, data stored on computer disk or by electronic means, which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format. *See* 18 U.S.C. § 2256(5).
- c. “Sexually Explicit Conduct” refers to actual or simulated (a) sexual intercourse (including genital-genital, oral-genital, anal-genital or oral-anal), whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).
- d. “Child Erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily, in and of themselves, obscene or that do not necessarily depict minors in sexually explicit poses or positions.
- e. “Minor” means any person under the age of eighteen years. *See* 18 U.S.C. § 2256(1).
- f. “Internet Service Providers” or “ISPs” are commercial organizations which provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers, including access to the Internet, web hosting, e-

mail, remote storage, and co-location of computers and other communications equipment.

- g. Internet Protocol Address” or “IP Address” is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.
- h. The “Secure Hash Algorithm” (SHA) was developed by the National Institute of Standards and Technology (NIST), along with the National Security Agency (NSA), as a means of identifying files using a digital “fingerprint” that consists of a unique series of letters and numbers. The United States has adopted the SHA1 hash algorithm as a Federal Information Processing Standard. SHA1 is the most widely used of the existing SHA hash functions, and is employed in several widely used applications and protocols. A file processed by this SHA1 operation results in the creation of an associated hash value often referred to as a digital signature. SHA1 signatures provide a certainty exceeding 99.99% that two or more files with the same SHA1 signature are identical copies of the same file regardless of their file names.
- i. “Computer” means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility

directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device. *See* 18 U.S.C. § 1030(e)(1).

- j. “Storage Medium” means any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.
- k. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including, but not limited to, central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including, but not limited to, keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including, but not limited to, physical keys and locks).
- l. “Computer passwords and data security devices” consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to “unlock” particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data

security software of digital code may include programming code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

- m. “Computer software” is digital information that can be interpreted by a computer and any of its related components to direct the way it works. Computer software is stored in electronic, magnetic, or other digital form. It commonly includes programs to run operating systems, applications, and utilities.
- n. “Records” and “Information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

BACKGROUND ON THE INTERNET, COMPUTERS, AND CHILD PORNOGRAPHY

8. Based on my knowledge, experience, and training and the experience and training of other law enforcement officers who routinely conduct child pornography investigations with whom I have had discussions, computers and the Internet have revolutionized crimes involving child pornography. Computers serve multiple functions in connection with child pornography crimes including: a means of producing, distributing, receiving and storing child pornography and a means of communicating with other offenders and enticing victims.

9. Today, the majority of computers manufactured for personal use come equipped with a camera enabling the user to produce images and videos. Thus, using computers, child

pornographers are readily able to produce, or request that minor victims create child pornography. Further, images and videos created using digital cameras can easily be transferred directly to a computer. Using a scanner, computers have the ability to convert traditional non-digital photographic images into a digital format thereby enabling the digitalization of child pornography produced using a film camera.

10. Individuals interested in the sexual exploitation of children may also use technology to target minors, interact with minors, and entice minors to produce child pornography. This is often accomplished through the use of social networking applications such as Facebook, Instagram, Kik Messenger, Musical.ly, and LiveMe.

11. The ability of computers and electronic storage media to store large amounts of digital files makes them ideal repositories for child pornography. The capacity of these devices to store digital information has grown tremendously within the last several years enabling the storage of thousands of images and videos at very high resolutions.

12. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, a computer user can contact literally millions of other users around the world. The Internet affords collectors of child pornography multiple methods for storing, obtaining, distributing, and/or viewing child pornography in a relatively secure and anonymous fashion. These methods include, but are not limited to, email, instant messaging services, websites, social media applications, cloud storage services, message boards, and peer-to-peer file sharing networks (P2P). These same means enable those involved with child pornography to communicate with like-minded offenders and minor victims. Even in cases where cloud storage is used, evidence of child pornography can be found on the user's computer or external media in most cases.

13. Mobile devices, hand-held computers, can transfer media through multiple methods – cellular signal, Wi-Fi, Bluetooth, and near field communication (NFC). In addition, mobile devices are commonly set to backup automatically when connected to a computer. Individuals have been known to plug their mobile devices into computers causing data to be backed up to the computer without even realizing that this data transfer is occurring. Mobile devices can also be set to sync automatically with cloud storage and paired devices. For example, an individual using Google Pictures or iCloud Photo Library may have images taken using a mobile device automatically backup to cloud storage and pushed out to, or “synced,” with their other computer devices.

14. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files). Digital information can also be retained unintentionally such as the traces of the path of an electronic communication may be automatically stored in many places (*e.g.*, application data, temporary files or ISP client software, among others). In addition, to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

15. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the internet (*e.g.*, tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior

versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

THE BITTORRENT PEER-TO-PEER NETWORK

16. Based on my training, experience, and information communicated to me by other law enforcement officers knowledgeable in the area, I know that millions of computer users throughout the world use peer-to-peer (P2P) file sharing networks to share files containing music, graphics, movies, and text. These networks have also become a popular way to download and distribute child pornography. Any computer user who can connect to the Internet can download P2P application software, which is typically free, and use it to share files through a P2P network.

17. The BitTorrent network is a publicly available P2P file sharing network. Most computers that are part of this network are referred to as “peers” or “clients.” A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients.

18. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, examples of which include the BitTorrent client program, µTorrent client program, and Vuze client program, among others. These client programs are publicly available and typically free software programs that can be downloaded from the Internet.

19. During the installation of typical BitTorrent network client programs, various settings are established which configure the host computer to share files via automatic uploading. This is commonly referred to as “passive distribution.”

20. As an example, during the downloading and installation of the publicly available μ Torrent client program, the license agreement for the software states the following: “Automatic Uploading. μ Torrent accelerates downloads by enabling your computer to grab pieces of files from other μ Torrent or BitTorrent users simultaneously. Your use of the μ Torrent software to download files will, in turn, enable other users to download pieces of those files from you, thereby maximizing download speeds for all users. In μ Torrent, only files that you are explicitly downloading or sharing (seeding) will be made available to others. You consent to other users’ use of your network connection to download portions of such files from you. At any time, you may uninstall μ Torrent through the Add/Remove Programs control panel utility. In addition, you can control μ Torrent in multiple ways through its user interface without affecting any files you have already downloaded.”

21. Typically, as users download files or pieces of files from other peers/clients on the BitTorrent network, other users (peers/clients) on the network are able to download the files or pieces of files from them, a process which maximizes the download speeds for all users on the network. Once a user has completed the download of an entire file or files, they can also continue to share the file with individuals on the BitTorrent network who are attempting to download all pieces of the file or files, a process referred to as “seeding.”

22. Files or sets of files are shared on the BitTorrent network via the use of “Torrents.” A “Torrent” is typically a small file that describes the file(s) to be shared. It is important to note that “Torrent” files do not contain the actual file(s) to be shared, but

information about the file(s) to be shared. This information includes things such as the name(s) of the file(s) being referenced in the “Torrent” and the “info hash” of the “Torrent.” The “info hash” is a SHA1 hash value of the set of data describing the file(s) referenced in the “Torrent.” This set of data includes the SHA1 hash value of each file piece in the torrent, the file size(s), and the file name(s). The “info hash” of each “Torrent” uniquely identifies the “Torrent” file on the BitTorrent network. The “Torrent” file may also contain information on how to locate file(s) referenced in the “Torrent” by identifying “Trackers.” “Trackers” are computers on the BitTorrent network that collate information about the peers/clients that have recently reported they are sharing the file(s) referenced in the “Torrent” file. A “Tracker” is only a pointer to peers/clients on the network who may be sharing part or all of the file(s) referenced in the “Torrent.” “Trackers” do not actually have the file(s) but are used to facilitate the finding of other peers/clients that have the entire file(s) or at least a portion of the file(s) available for sharing.

23. It should also be noted that the use of “Tracker(s)” on the BitTorrent network are not always necessary to locate peers/clients that have file(s) being shared from a particular “Torrent” file. There are many publicly available servers on the Internet that provide BitTorrent tracker services.

24. In order to locate “Torrent” files of interest and download the files that they describe, a typical user will use keyword searches on torrent indexing websites, examples of which include isohhunt.com and thepiratebay.org. Torrent indexing websites are essentially search engines that users on the BitTorrent network use to locate “Torrent” files that describe the files they are looking to download. Torrent indexing websites do not actually host the content (files) described by “Torrent” files, only the “Torrent” files themselves. Once a “Torrent” file is

located on the website that meets a user's keyword search criteria, the user will download the "Torrent" file to their computer. The BitTorrent network client program on the user's computer will then process that "Torrent" file in order to find "Trackers" or utilize other means that will help facilitate finding other peers/clients on the network that have all or part of the file(s) referenced in the "Torrent" file.

25. It is again important to note that the actual file(s) referenced in the "Torrent" are obtained directly from other peers/clients on the BitTorrent network and not the "Trackers" themselves. Typically, the "Trackers" on the network return information about remote peers/clients that have recently reported they have the same file(s) available for sharing (based on SHA1 "info hash" value comparison), or parts of the same file(s), referenced in the "Torrent," to include the Internet Protocol (IP) addresses of the remote peers/clients.

26. For example, a person interested in obtaining child pornographic images or videos on the BitTorrent network can go to a torrent indexing website and conduct a keyword search using a term such as "preteen sex" or "pthc" (pre-teen hardcore). The results of the keyword search are typically returned to the user's computer by displaying them on the torrent indexing website. Based on the results of the keyword search, the user would then select a "Torrent" of interest to them to download to their computer from the website. Typically, the BitTorrent client program on their computer will then process the "Torrent" file. Utilizing trackers and other BitTorrent network protocols, peers/clients would then be located that have recently reported they have the file(s) or parts of the file(s) referenced in the "Torrent" file available for sharing. The file or files are then downloaded directly from the computer(s) sharing the file or files to the user's computer.

27. Typically, once the BitTorrent network client has downloaded part of a file or files, it will immediately begin sharing the part of the file or files it has with other users on the network. The BitTorrent network client program succeeds in reassembling the file(s) from different sources only if it receives “pieces” with the exact SHA1 piece hash described in the “Torrent” file. The downloaded file or files are then stored in an area (folder) previously designated by the user and/or the client program on the user’s computer or designated external storage media. The downloaded file or files, including the torrent file, will remain in that location until moved or deleted by the user.

28. Law enforcement efforts have resulted in the creation of BitTorrent network client programs that obtain information from “Trackers” about peers/clients on the BitTorrent network involved in sharing digital files of known or suspected child pornography. This is accomplished using based on “info hash” SHA1 hash values of “Torrents” which have been previously identified by law enforcement as being associated with such files. The law enforcement BitTorrent network client programs are designed to perform single-source downloads of files. In other words, entire files are downloaded from a single computer at a single IP address.

29. During the query and/or downloading process from a suspect BitTorrent network client, certain information may be shared by the suspect client program with the law enforcement BitTorrent client program. This information includes 1) the suspect client’s IP address; 2) a confirmation from the suspect client that they have pieces of the file(s) being requested, and that the pieces are being reported as shared from the suspect client program; and 3) the BitTorrent network client program and version being utilized by the suspect computer.

30. The investigation of P2P file sharing networks is a cooperative effort of law enforcement agencies around the country. Many of these agencies are associated with the

Internet Crimes against Children (ICAC) Task Force Program. P2P investigative methodology has led to the issuance and execution of search warrants around the country resulting in the arrest and conviction of numerous offenders possessing and/or distributing child pornography, some of which were also involved in the active hands-on sexual exploitation of actual children.

PROBABLE CAUSE

31. Between January 14, 2022 to January 24, 2022, an Online Covert Employee (OCE) with the FBI Charlotte Field Office Crimes Against Children and Human Trafficking (CACHT) Task Force was utilizing a BitTorrent application to conduct undercover investigations into the sharing of child sexual abuse material (CSAM)¹ on the BitTorrent peer-to-peer (“P2P”) file sharing network. During the investigation, the OCE identified a computer that may contain investigative files of interest. The files had been identified by conducting keyword or hash value searches of files related to CSAM on the BitTorrent network.

32. Between January 14, 2022 to January 24, 2022, an OCE downloaded numerous files depicting minors engaged in sexually explicit conduct directly from IP address 174.111.33.18. The following are five of the files downloaded:

- a. A video titled, **“!!! NEW !!! 2010 kait 5yo - chunk2 FK pthc best.avi”** that is approximately 00:01:25 in length, shows an adult male engaging in vaginal

¹ By accepted best practice, the term “child pornography” will hereafter be referred to in this affidavit as “child sexual abuse material” or CSAM, which law enforcement, court officials and survivors agree better reflects the gravity of this criminal offense.

intercourse with a prepubescent minor female, who appears to be under the age of 6.

- b. A video titled, "**10 yo KAJ R@YGOLD BABY RAPE - PLEASE SHARE!!! clip fr dadndotr 10yo play in woods 2.03(pthc pedo kiddy incest).mpg**" that is approximately 00:02:03 in length, shows a fully nude adult male with a fully nude prepubescent minor female, who appears to be under the age of 10 in a wooded setting. The adult male flips the minor over while standing up. The prepubescent minor female is observed masturbating the adult male prior to the adult male laying down on a blanket. The prepubescent minor female straddles over top of the adult male and engages in vaginal intercourse. Before the video ends, the prepubescent minor female is observed straddling over top of the adult male's face in which he performs oral sex on her.
- c. A video titled, "**PTHC NEW Baby Nice Orgasm From 4yo Girl 2011.mpg**" that is approximately 00:04:09 in length, shows a heavily bearded adult male with "sleeve-style" tattoos sitting with a clothed prepubescent minor female, who appears to be under the age of 4. She is wearing a shirt with underwear and has a pacifier in her mouth. As the video progresses, the adult male pulls aside the prepubescent minor female's underwear, displaying her genitals in a lewd and lascivious manner and digitally penetrates her vagina.
- d. A video titled, "**!!! NEW Pthc - 0607!!! kelly - 7yo backyard fuck & pedo kittycum.mpg**" that is approximately 00:03:52 in length, shows a prepubescent minor female, who appears to be under the age of 7, fully clothed in a backyard

setting. As the video progresses, the prepubescent minor female is observed fully nude and displaying her genitals in a lewd and lascivious manner. An adult male is observed masturbating at her vagina and proceeds to ejaculate on her genitals.

- e. A video titled, "**pthc 9yo webcam little girl show pussy finger no hymen (new 2011).avi**" that is approximately 00:04:25 in length, shows a prepubescent minor female, who appears to be under the age of 9, displaying her vagina and anus in a lewd and lascivious manner. She is observed digitally penetrating both her vagina and anus. The video appears to be a recording of a monitor playing the above described acts.

33. On January 25, 2022, Special Agent (SA) Michael Gregory queried Internet Protocol ("IP") address 174.111.33.18 through arin.net which showed it was registered with Charter Communications, Inc. The same day, SA Gregory served an Administrative Subpoena to Charter Communications, Inc for subscriber information pertaining to IP address 174.111.33.18.

34. On February 2, 2022, SA Gregory received via a web portal, records from Charter Communications, Inc. reference IP address 174.111.33.18. Records showed the IP address belongs to the below:

Full Name: Madi Markulik
Address: 2657 Ben Joyce Road Kernersville, NC 27284-9690
Phone number: (336) 757-2779
User Name: MPMARKULIK@hotmail.com
Current Lease Start: November 22, 2020 02:06 PM Eastern

35. According to open-source records checks, Madi Markulik HASSLER resides at 2657 Ben Joyce Road, Kernersville, North Carolina with her husband, Matthew HASSLER.

36. On March 8, 2022, a search warrant was issued out of the United States District Court for the Middle District of North Carolina for the residence at 2657 Ben Joyce Road, Kernersville, North Carolina in reference to violations of Title 18, United States Code, Section 2252A(a)(2)(A) and Title 18, United States Code, Section § 2252A(a)(5)(B). On March 10, 2022, the FBI served the search warrant at the residence. Prior to the service of the warrant, Matthew HASSLER was observed leaving the residence. HASSLER drove to his employment located at Grass America, Inc., 1202 NC-66, Kernersville, North Carolina 27284.

37. HASSLER was consensually interviewed at Grass America by FBI and Forsyth County Sheriff's Office investigators. HASSLER was advised of an FBI investigation and wanted to ask him a couple of questions. He was given the option to speak with Agents in an FBI vehicle and chose to speak inside the vehicle. During the interview, HASSLER admitted to viewing CSAM online since he was younger. He admitted it was a clear problem and had downloaded BitTorrent onto a laptop a couple of months ago. The passcode for the laptop was 1191. He said that while in BitTorrent, he found a folder on an onion site with instructions. He followed the instructions and opened and viewed the file which contained approximately 50 videos of CSAM. He described the content of the videos primarily containing female minors, ages ranging from infant to pubescent. HASSLER said his preference of CSAM is females between 12-15 years of age. After viewing CSAM, HASSLER said he would delete the files. HASSLER said he has a problem, doesn't have access to minors, but intentionally decided not to have children because he didn't know what he would do. HASSLER identified his email address as chargerzx11@gmail.com.

38. HASSLER said he had the Device on him during the interview and provided the passcode. When asked for consent to search the Device, HASSLER declined and requested to speak with an attorney.

39. During the service of the search warrant at the residence, a Dell Inspiron laptop Model P30E was located on the kitchen table. The passcode to get into the laptop was 1191. A cursory search of the laptop yielded the BitTorrent and Tor browsers on the desktop of user, “charg.”

40. During the service of the search warrant at the residence, a 320GB Western Digital hard drive, serial number WXG1AB0T8436 was located in a bedroom. Several files containing CSAM were located on the hard drive in the “Downloads” folder under the user folder “charg.” A summary of the some of the files follows:

- a. An image titled “**KS01-39.jpg**” shows a prepubescent minor female’s midsection that displays her vagina. An adult is seen exposing the minor’s vagina in a lewd and lascivious manner.
- b. An image titled “**KX01-09.jpg**” shows a prepubescent minor female’s rear midsection with her underwear pulled down. An adult is seen exposing the minor’s anus in a lewd and lascivious manner.
- c. An image titled “**KS01-25.jpg**” shows a prepubescent minor female laying down with her eyes closed and apparently asleep. An adult male’s penis is close to her face; a clear, milky substance is observed on the face of the prepubescent minor female’s face. A caption on the image says, “LOOK AT THAT !! JoeY shoots his entire load on Inga lips – the first cum ever on Inga, right in her face – on her

mouth!! Inga m cans and turn her head a bit, I wonder what she dreams...

Someting tasy, I believe.”

- d. An image titled “**KS01-12.jpg**” shows a topless, prepubescent female holding an adult male’s penis. laying down with her eyes closed and apparently asleep. A caption on the image says, “Slowly and with a gentle grip, she pulls back the foreskin...”
 - e. An image titled “**KS01-17.jpg**” shows a topless, prepubescent female with her lips on an adult male’s penis. A caption on the image says, “My head spins at the sight of Ingas’ lips touching another mans’ cock!! She keeps on kissing and kissing, and JoeY starts to wank....”
41. After HASSLER’s initial interview at Grass America, Inc. and when he requested to speak with an attorney, HASSLER asked to go back to his residence. HASSLER drove his car back to his residence. Following his arrival back at the residence, HASSLER was detained and subsequently arrested on suspicion of CSAM related offenses. HASSLER was carrying his car keys and the Device in his hands prior to be detained; the Device was subsequently seized.
42. The Device is currently in storage at FBI Charlotte located at 7915 Microsoft Way, Charlotte, North Carolina 28273. In my training and experience, I know that the Device has been stored in a manner in which its contents are, to the extent material to this investigation, in substantially the same state as they were when the Device first came into the possession of the FBI.

TECHNICAL TERMS

43. Based on my training and experience, I use the following technical terms to convey the following meanings:

- a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional “land line” telephones. A wireless telephone usually contains a “call log,” which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic “address books;” sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system (“GPS”) technology for determining the location of the device.
- b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by

connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

- c. **Portable media player:** A portable media player (or “MP3 Player” or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.
- d. **GPS:** A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated “GPS”) consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that

are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

- e. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.
- f. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

- g. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

44. Based on my training, experience, and research, I know that the Device has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS, and Tablet, to utilize an IP Address and to connect to the Internet. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

45. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

46. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the Device was used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on the Device because:

- a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).
- b. Forensic evidence on a device can also indicate who has used or controlled the device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence.
- c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.
- d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.
- e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

47. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

48. *Manner of execution.* Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

49. I submit that this affidavit supports probable cause for a search warrant authorizing the examination of the Device described in Attachment A to seek the items described in Attachment B.

Respectfully submitted,

/s/ Michael Gregory
Michael Gregory
Special Agent
Federal Bureau of Investigation

This Affidavit was reviewed by AUSA Cortney Randall

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 18th day of March, 2022, at 4:08 PM.

Signed: March 18, 2022



W. Carleton Metcalf
United States Magistrate Judge



ATTACHMENT A

The property to be searched is a Samsung SM-G998U cellular phone, serial: R3CR70HDQN[last alphanumeric character illegible], IMEI 1: 351600220114740, IMEI 2: 350876360114747, hereinafter the “Device.” The Device is currently located at 7915 Microsoft Way, Charlotte, North Carolina 28273.

This warrant authorizes the forensic examination of the Device for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

ITEMS TO BE SEARCHED AND SEIZED

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. Computer or storage media that could be used as a means to commit the violations described above including the DEVICE described in Attachment A.
2. For the computer or storage medium whose seizure is otherwise authorized by this warrant (hereinafter, “the DEVICE”):
 - a. evidence of who used, owned, or controlled the DEVICE at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
 - b. evidence of software that would allow others to control the DEVICE, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
 - c. evidence of the lack of such malicious software;

- d. evidence of how, when and where the DEVICE was accessed or used to determine the chronological context of computer access, use, and events relating to the crimes under investigation and to the DEVICE's user;
 - e. evidence of the attachment to the DEVICE of other storage devices or similar containers for electronic evidence;
 - f. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the DEVICE;
 - g. evidence of the times the DEVICE was used;
 - h. records of or information about Internet Protocol addresses used by the DEVICE;
 - i. records of or information about the DEVICE's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
 - j. contextual information necessary to understand the evidence described in this attachment;
- 3. Child pornography, as defined in 18 U.S.C. § 2256(8);
 - 4. Child erotica;
 - 5. Visual depictions used to generate child pornography or child erotica;
 - 6. Records, information, and items relating to violations of the statutes described above in the form of:
 - a. Records or documents evidencing use or ownership of the DEVICE, including utility and telephone bills, email or addressed correspondence;

- b. Records and information referencing or revealing the sexual exploitation of children and/or trafficking of child pornography;
- c. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence;
- d. Records and information referencing or revealing the use of remote computing services such as email, cloud storage or online social media services; and
- e. Records or information referencing or revealing the use of peer-to-peer software, including BitTorrent client software.

As used above, the terms “records” and “information” includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

This warrant authorizes a review of electronic storage media and electronically stored information seized or copied pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine (“protected materials”), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.